Securing Data at Rest : Protect Applications, DataBases, Files, and Cloud Data

Ugo Piazzalunga

Pre-sales Manager, Southern Region, EMEA

ugo.piazzalunga@safenet-inc.com

Agenda

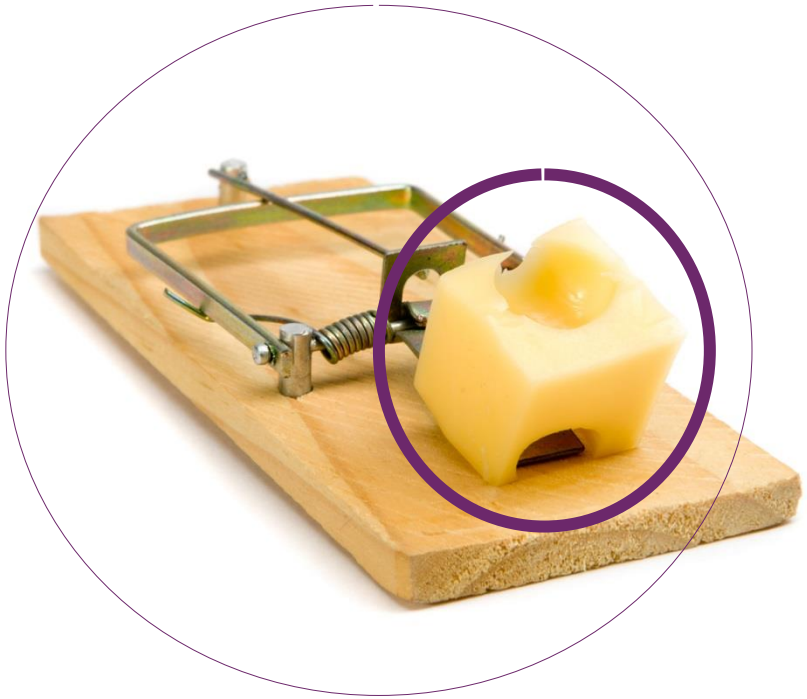
- Data breaches – a Given!
- The need for a different approach to data protection
- The Technology: Cryptography
- SafeNet Data Encryption portfolio
- Use Cases
- Compliance mandates

SafeNet. THE DATA PROTECTION COMPANY

Protect the target, not the perimeter

or

Protect the CHEESE, not (just) the mousetrap



SafeNet. THE DATA PROTECTION COMPANY

The best technology to protect data (the cheese)

Cryptography

provides

- Confidentiality
- Authenticity
- Integrity
- Non-Repudiation

The best technology to protect data (the cheese)

Cryptography

provides

- Confidentiality
- Authenticity
- Integrity
- Non-Repudiation

PCI Security Standards Council

PCI DSS Requirements	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of*	**3.4.a** Exam the PAN, in encryption rendered u • One-wa • Truncat • Index to • Strong process **3.4.b** Exam repositories not stored i **3.4.c** Exam back-up tap **3.4.d** Exam rendered u

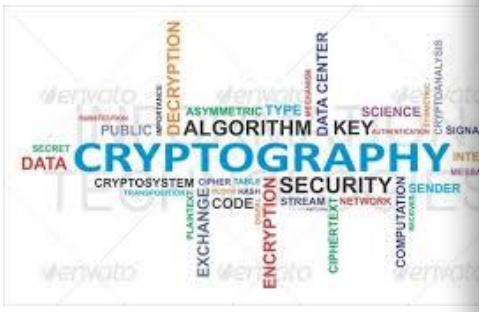
COMPANY

The best technology to protect data (the cheese)

Cryptography

provides

- Confidentiality
- Authenticity
- Integrity
- Non-Repudiation



L 173/2 EN Official Journal of the European Union

REGULATIONS

COMMISSION REGULATION (EU) No 611/2013

of 24 June 2013

on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

Article 4

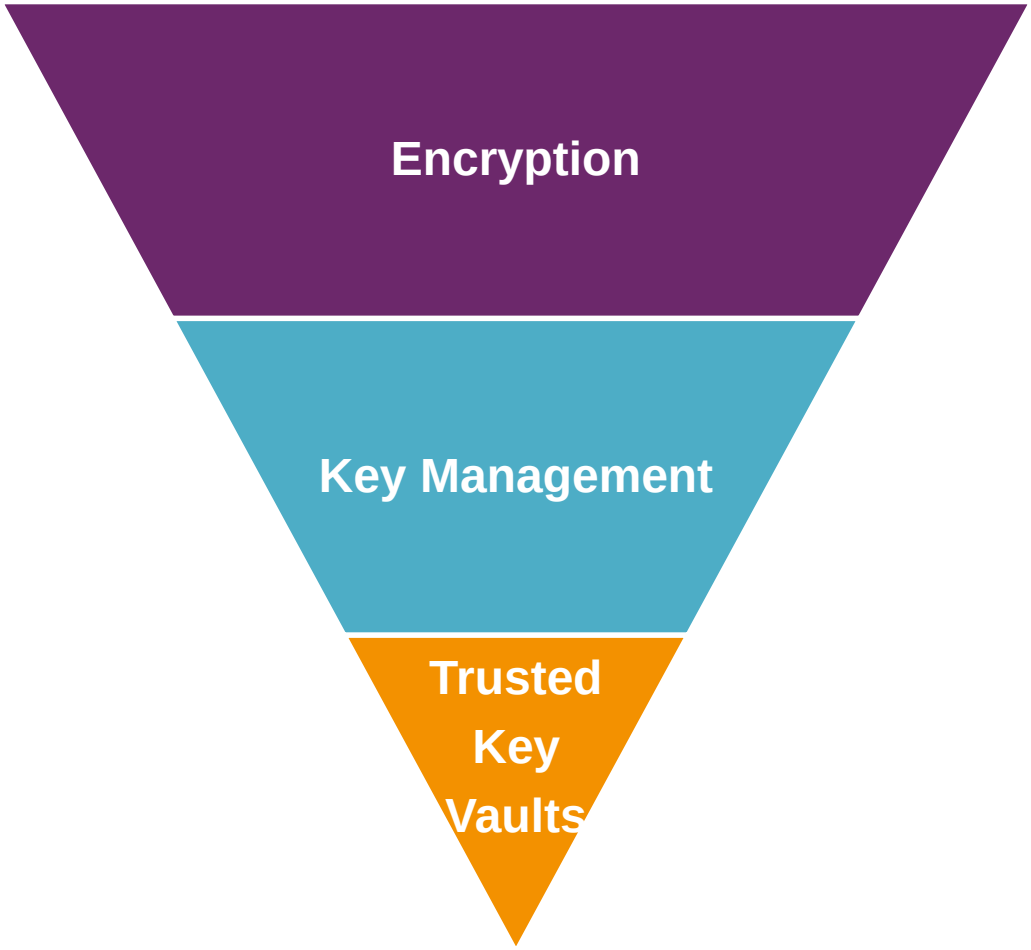
Technological protection measures

1. In derogation from Article 3(1), notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

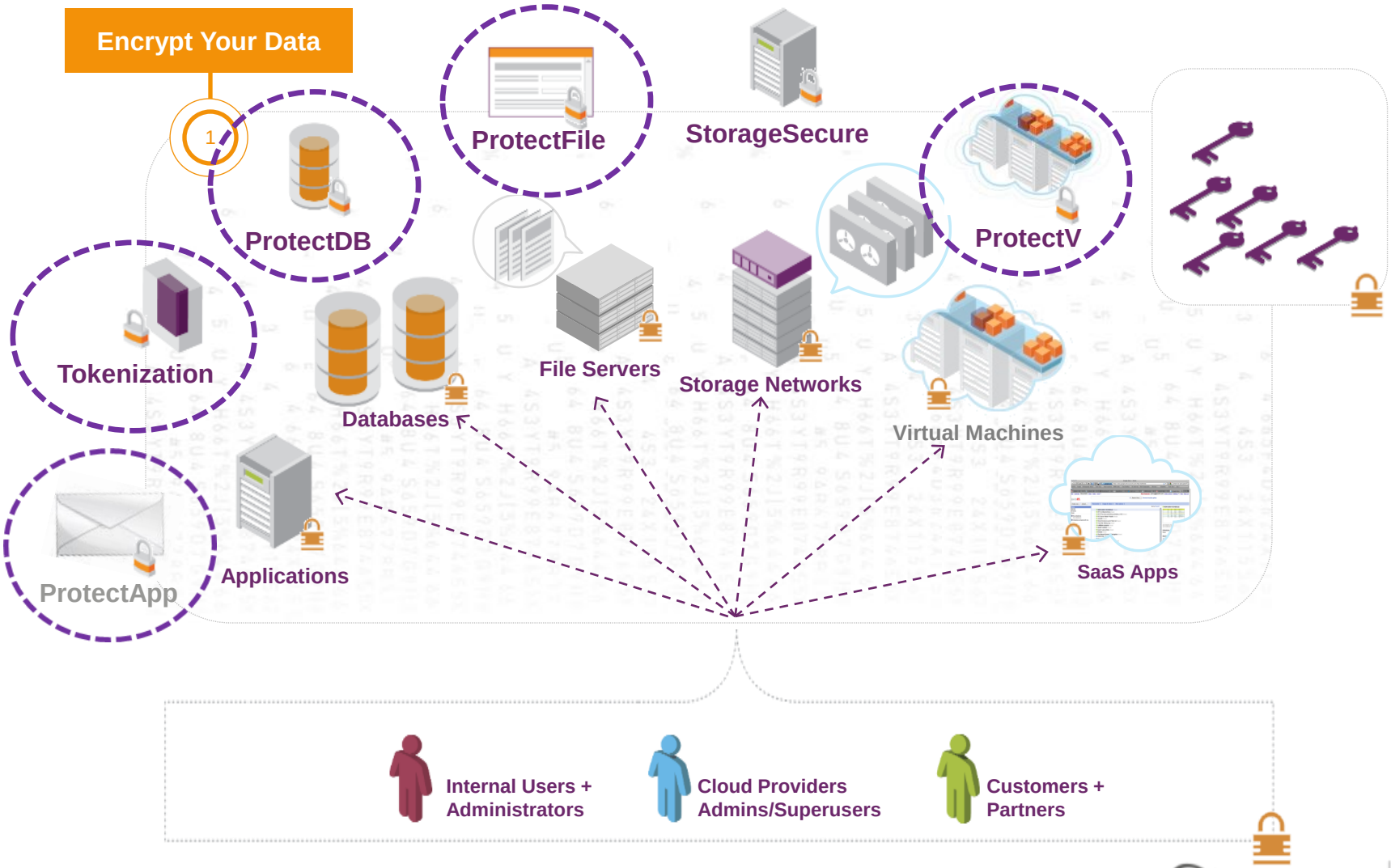
2. Data shall be considered unintelligible if:

(a) it has been securely encrypted with a standardised algorithm, the key used to decrypt the data has not been compromised in any security breach, and the key used to decrypt the data has been generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key; or

The Foundation of High Assurance Encryption



Protecting Your Data



SafeNet. THE DATA PROTECTION COMPANY

Protect Data at the Application Level

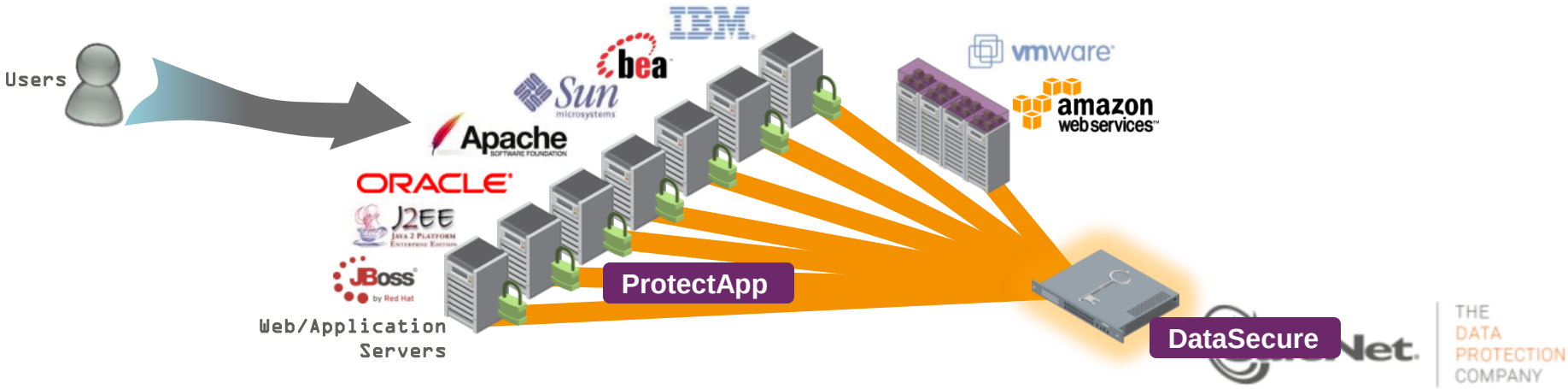
SafeNet ProtectApp

Benefits

- Removes performance impact on application servers
- Protects across multi-vendor application and development platforms
- Works with cloud deployed applications
- Faster time-to-deployment for encryption
- Enhances application security through fine-grained user controls

Features

- Application encryption with hardware appliance offload
- Supports all major application platforms
- Standard development libraries and APIs
  - .NET, ICAPI, JCE, MSCAPI, XML
- Supports applications in VMware and Xen
- Cryptographic management by DataSecure administrators
  - Supports delegated admin
- Granular user authentication policy: standard directory, DataSecure user, time of day, rate limiting, etc.



CASE STUDY

Key Management in the Digital Media Vertical

Challenge

- Central storage & management for crypto keys used by 10K servers
- Server authentication

Solutions and Outcome

- Security architecture based on ProtectApp + DataSecure – scalability, HA across multiple DCs, ProtectApp used by thousands of apps
- Centralized hardware-based key managements (DataSecure)
- Server authenticated through X509 certs and IP
- Automated key life-cycle processes (e.g. key rotations)
- Lower TCO, increased security

Transparent Database Protection

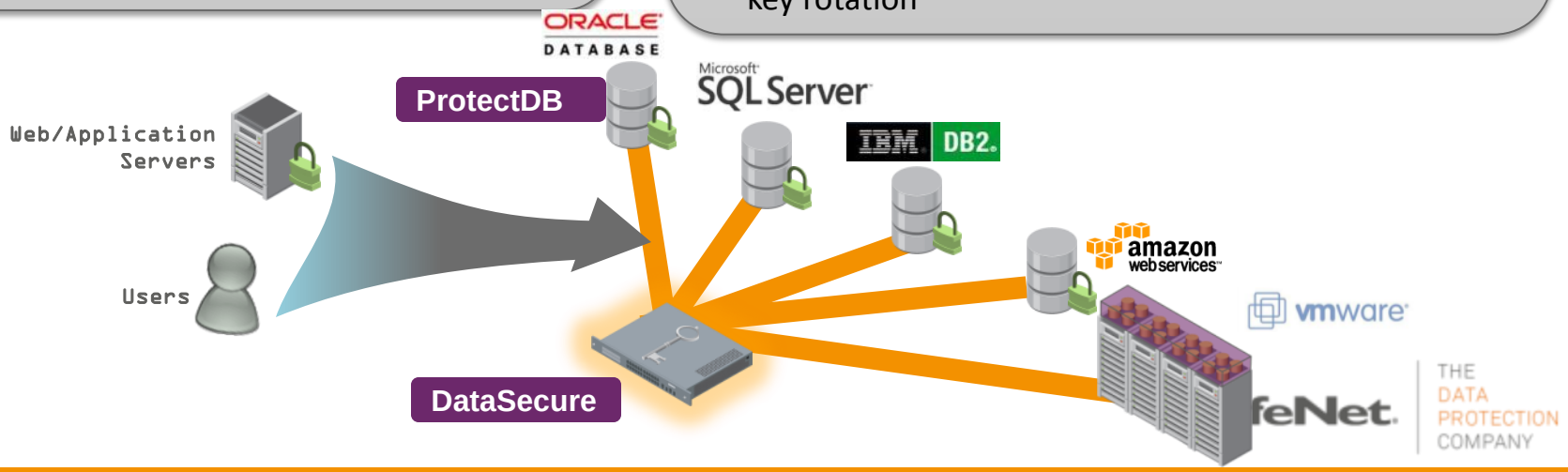
SafeNet ProtectDB

Benefits

- Removes performance impact on databases
- Protects across multi-vendor DBMS systems
- Application transparent
- Separation of duties from DB admins
- Centralized policy control of data access with granular restriction options
- Supports extremely large data sets
- Works with Cloud deployed databases

Features

- Column level database encryption with database offload
- DBMS Support: Oracle, MS SQL, DB2
- Automated view, trigger, and stored procedure generation
- Cryptographic management by DataSecure administrators
- Supports delegated admin
- Granular user authentication options: standard directory, DataSecure user, time of day, rate limiting, etc.
- Large data transformation support, including regular key rotation



CASE STUDY

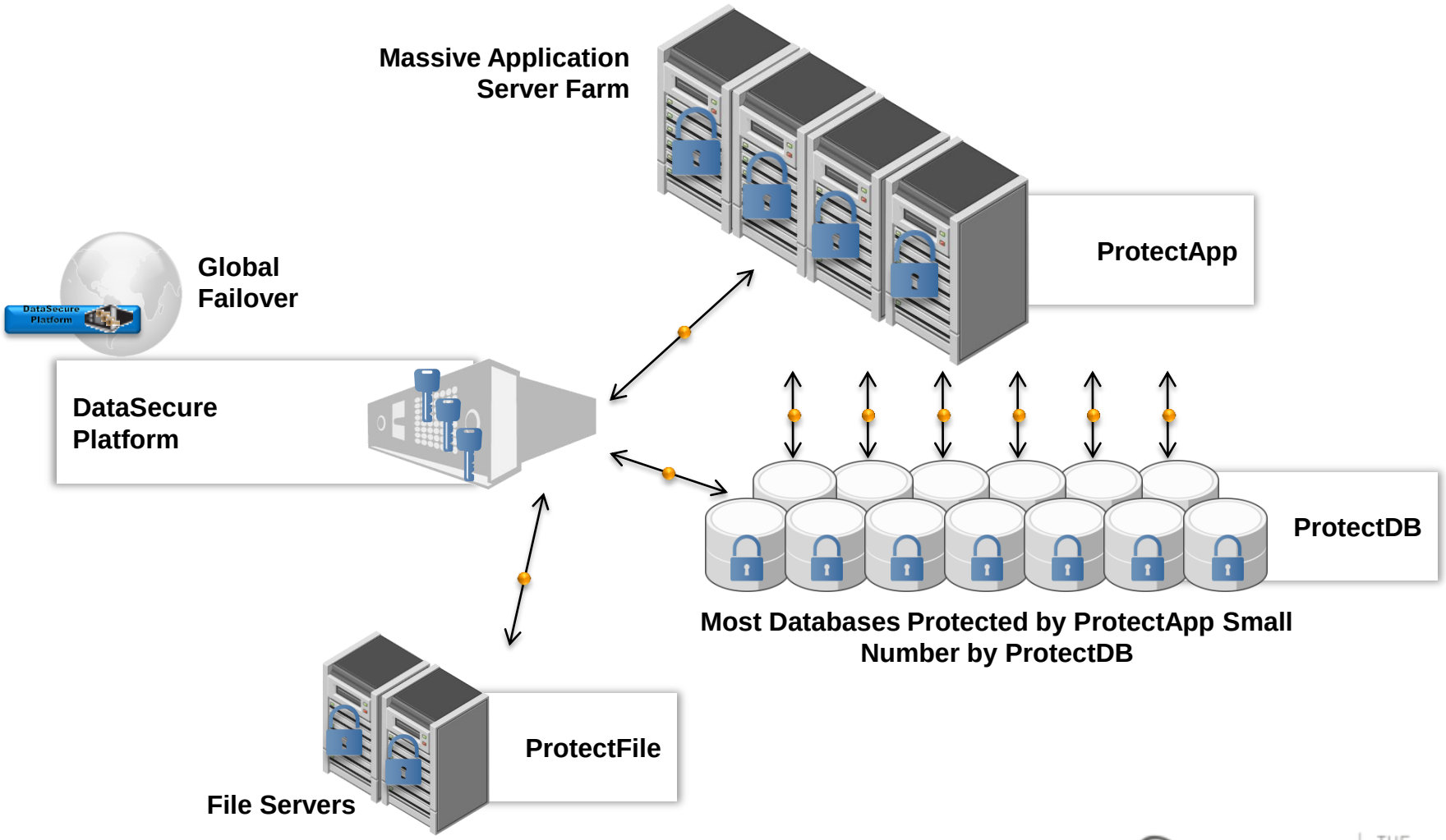
Compliance & Regulation for a large Global Online Merchant

- **Challenges**
  - Standardized security across a large number of databases and applications
  - After trying to deploy native 3rd party database encryption they decided to move to DataSecure
  - PCI DSS compliance and customer trust were the main drivers for encrypting data
- **SafeNet hardware/software products deployed**
  - 20+ DataSecure appliances for development, test, and production in multiple data centers
  - ProtectApp and ProtectDB across 120 servers
  - Starting to deploy ProtectFile
- **Outcome**
  - Encrypting over a million transactions per day
  - DataSecure is now the corporate standard for data protection
  - Work with SafeNet as a strategic partner for their future security needs

SafeNet. THE DATA PROTECTION COMPANY

CASE STUDY

Compliance & Regulation for a large Global Online Merchant



SafeNet. THE DATA PROTECTION COMPANY

Reducing PCI DSS Audit Scope:

SafeNet Tokenization Manager

Benefits

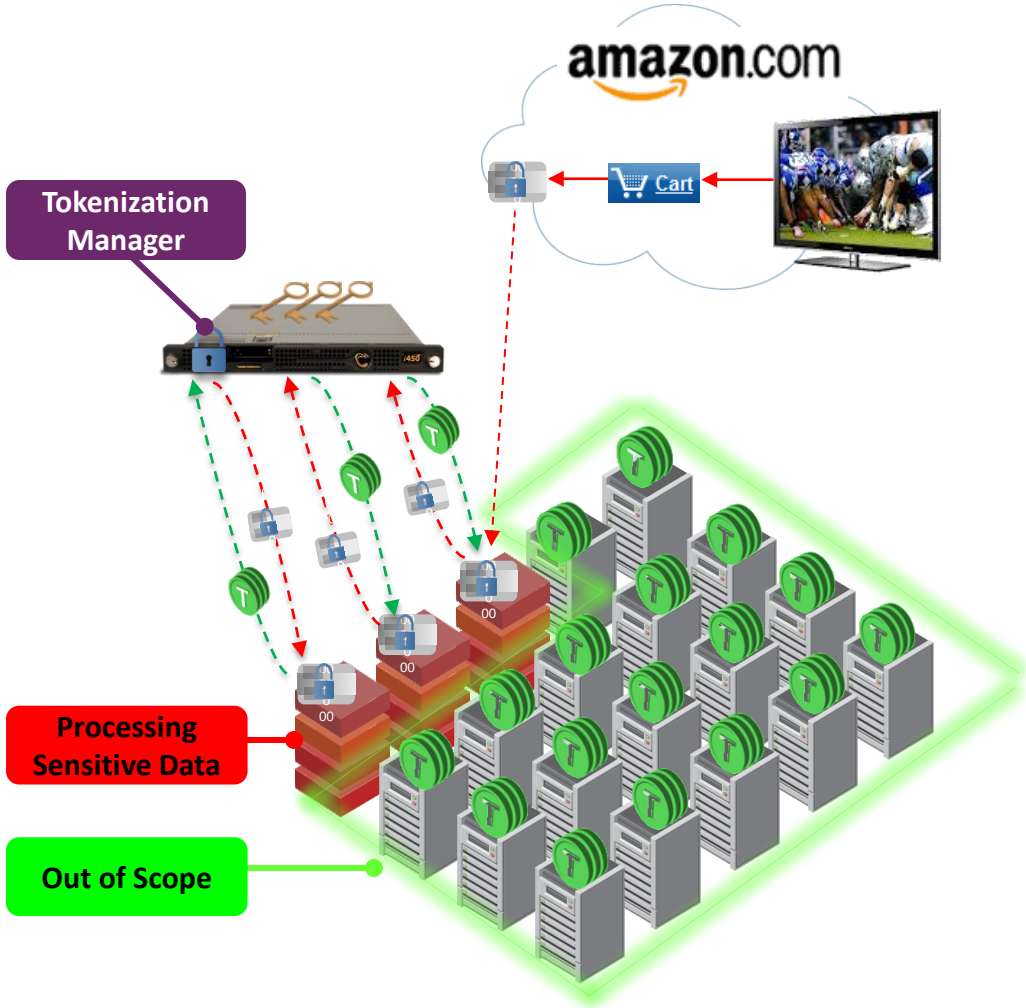
- Reduce scope of compliance audits such as PCI
- Transparent data protection–no changes to database tables, file layouts, or applications that don't handle clear data
- Enable strong protection of PANs and other data types without affecting business logic, database architecture, storage systems, or other critical enterprise components
- Replicate production data to test environments with no additional processing to de-identify or mask data
- Enables PCI DSS compliance through highly-secure enterprise key manager (DataSecure)

Features

- Replacement of sensitive data with data of a similar size that is not sensitive (a "token")

1410 5278 9923 4321

- 1-to-1 mapping of tokens to sensitive data
- Compliant with PCI DSS tokenization guidelines
- Integration through web services or Java and .NET APIs

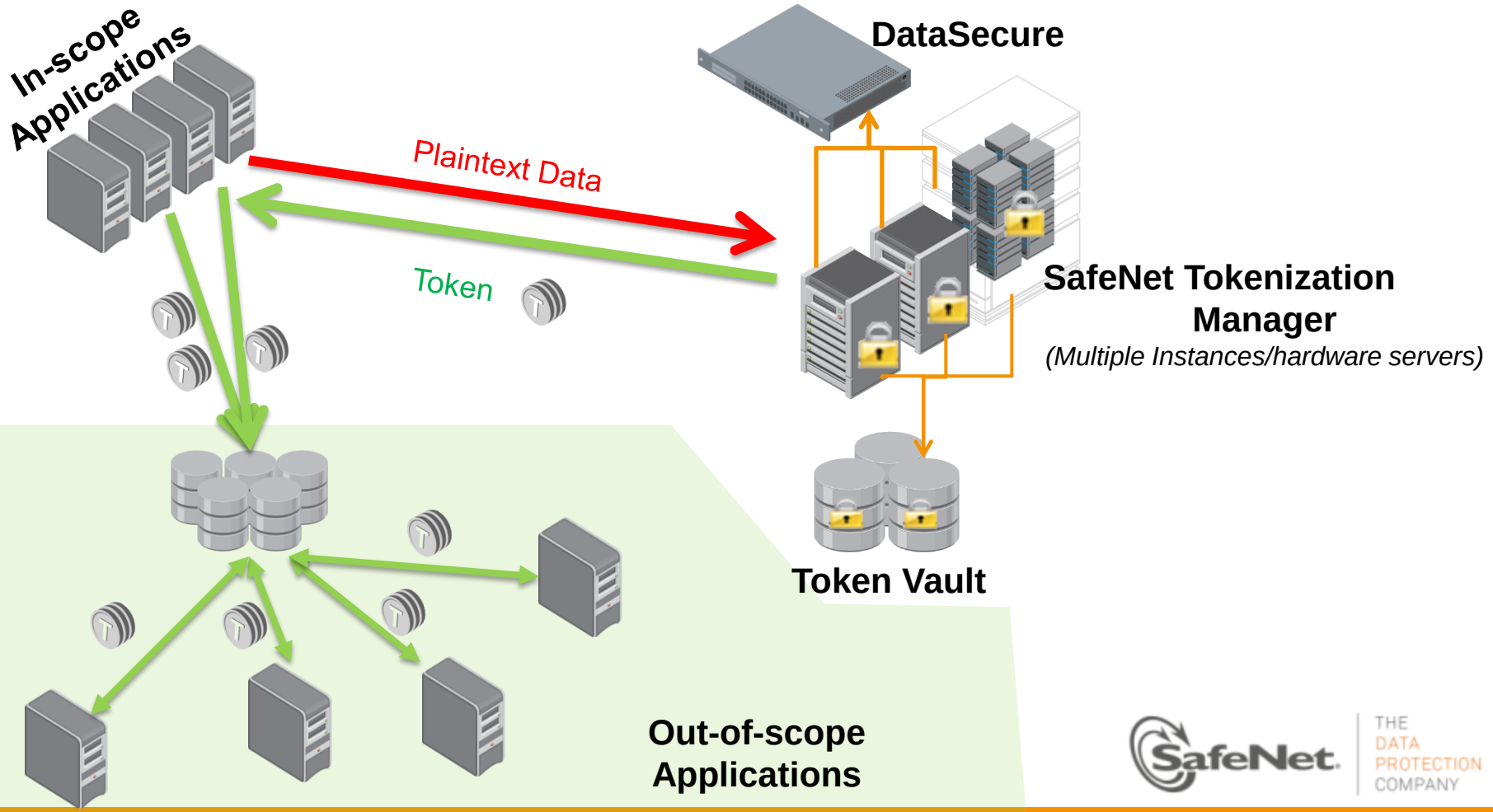


SafeNet. THE DATA PROTECTION COMPANY

CASE STUDY

Global leader for IT security & management solutions

→ Tokenization High level architecture



SafeNet. THE DATA PROTECTION COMPANY

CASE STUDY

Global leader for IT security & management solutions

→ Project Outcome

- Dramatic reduction of the PCI scope; Privacy PII ready
- Reduction of the audit cost (Quarterly pen tests, the number of IT assets subject to elevated security policies)
- Tokenization offered as a service to internal departments
- Can allow Token reuse across different departments
  - Management of tokens and data is now controlled to one team
  - Sensitive DataType examples: Usernames, Passwords, Credit Card, Account Numbers, Id numbers

Protect Unstructured Data in Files/Folders

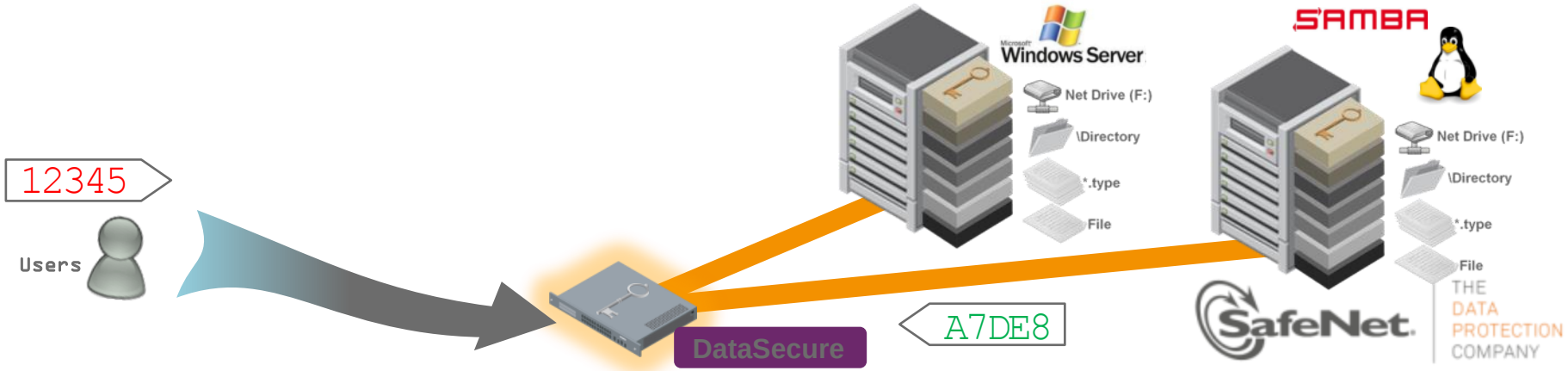
SafeNet ProtectFile

Benefits

- Comprehensive encryption for File Shares and Network Drives
- Transparent Operation
- Strong encryption with granular access controls
- Centralized, robust administration
- Easy deployment
- Large scale centralized key and policy management

Features

- File and folder encryption:
  - Physical , Virtual and network attached disks
  - Encryption keys stored and centrally managed in secure FIPS-certified hardware
  - Remote silent installation for easy deployment in any size environment
- Encryption algorithms - FIPS 140-2 strength AES algorithms
- Supported platforms - Microsoft Windows Server and Linux



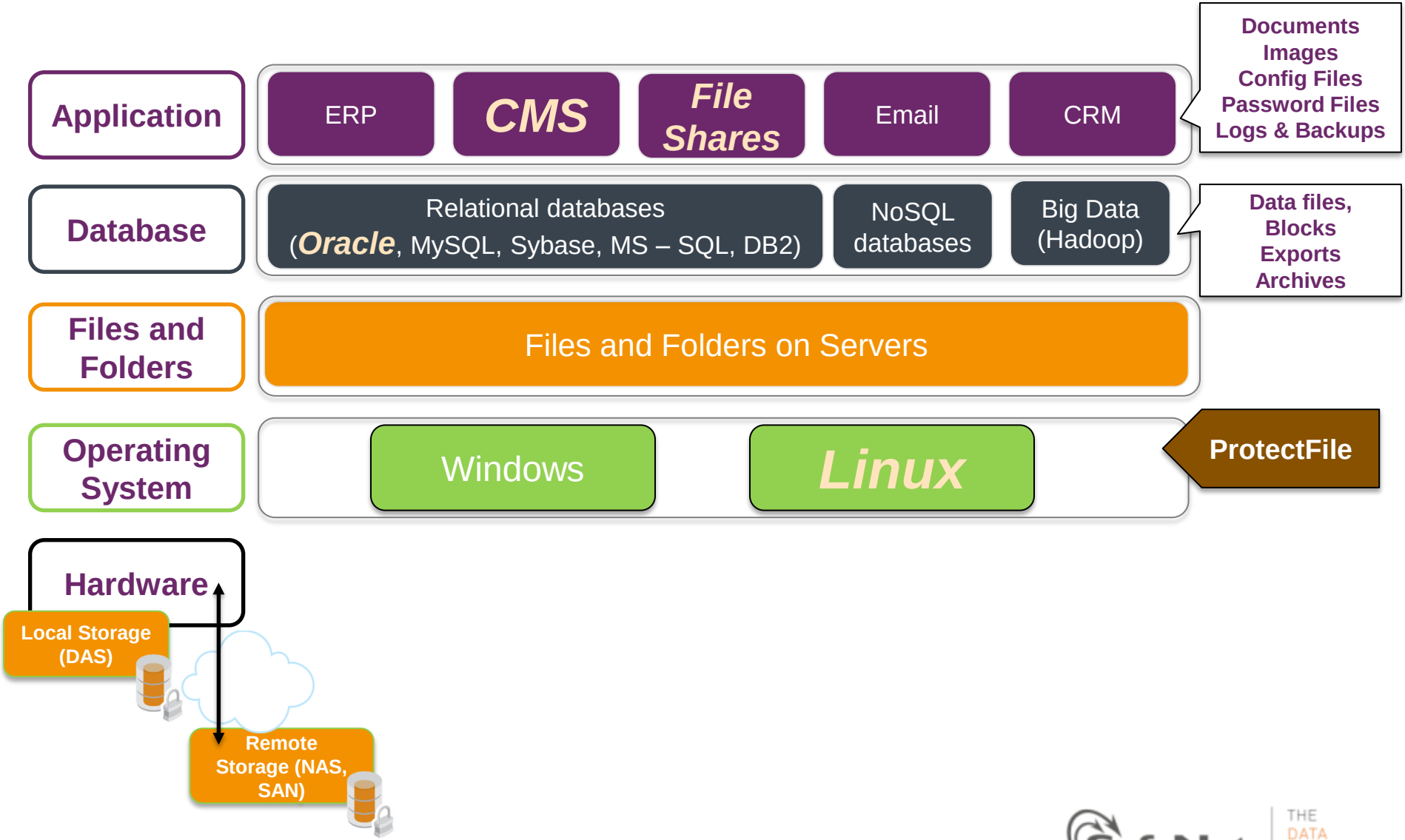
CASE STUDY

Protection of IPs in consumer electronics

Challenge

- Company's new products are highly sought-after
- Essential to keep secret the design work that precedes new product release
- Enables effective collaboration between various teams
  - Oracle content management system
  - Linux environment
  - Design documents in various unstructured formats
  - Protection without overcomplicating access to authorized users

ProtectFile Solution Scope



CASE STUDY

Protection of IPs in consumer electronics

→ Project Outcome

- **Growth enabled** - confident their sensitive data is secured, enabling focus on growing their business, securely
- **Collaboration secured** - only authorized, authenticated users can view sensitive unstructured data, enabling effective collaboration
- **Productivity empowered** - With transparent encryption, no disruption to business operations, performance, or end-user experience

ProtectV - Data Protection for the Cloud

ProtectV is the industry's first comprehensive **high-assurance** solution for **securing both virtual infrastructure and data.**

This gives you the freedom to migrate to virtual and cloud environments while maintaining full **ownership, compliance and control of data**.

vmware READY CERTIFIED

vmware PARTNER TECHNOLOGY ALLIANCE

amazon web services Partner Network
ADVANCED TECHNOLOGY PARTNER

SafeNet. THE DATA PROTECTION COMPANY

ProtectV: Secures the Entire VM Lifecycle

1 Provision

Every time that you provision VMs, ProtectV makes it efficient, fast, and automated

2 Start

You must be authenticated and authorized to launch a VM

3 Daily Operations

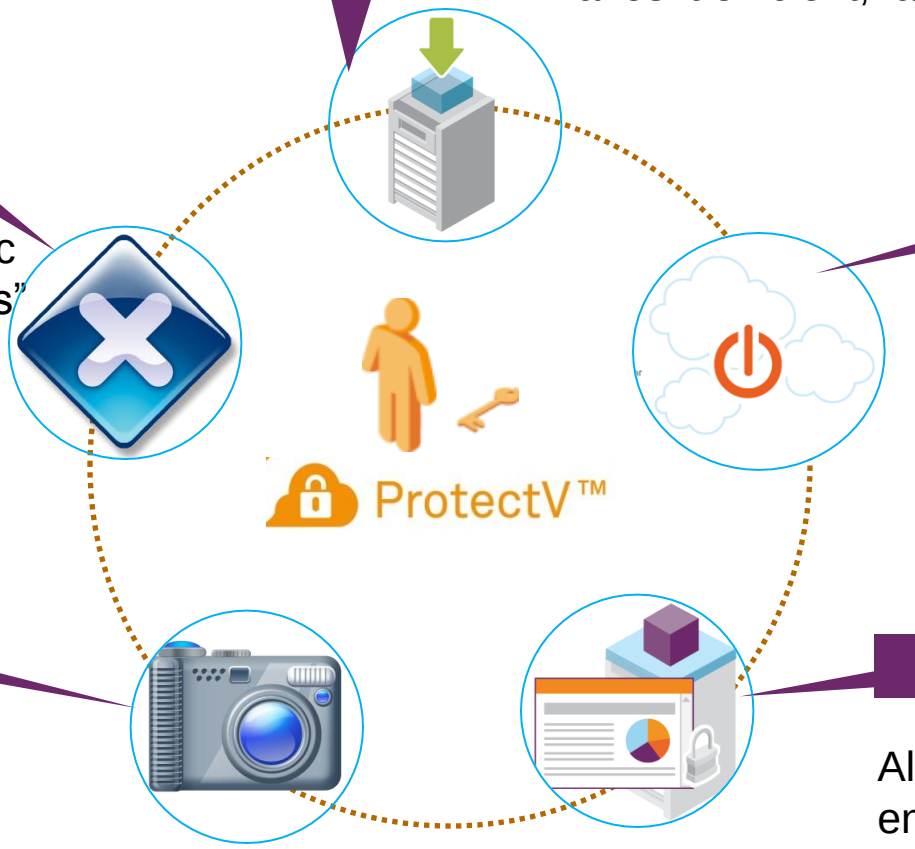
All data and VMs are encrypted

4 Snapshot

Every copy of VM in storage or backup is encrypted

5 Delete

Every time you delete a cryptographic key, it “digitally shreds” the data, rendering all copies of VMs inaccessible



SafeNet. THE DATA PROTECTION COMPANY

CASE STUDY

INFORMA - Multinational publishing & conference company

The Business Problem (Use Case)

- Moving physical datacenter into the public cloud – Amazon Virtual Private Cloud (VPC)
- Using Infrastructure as a Service
- All virtual servers hosted in Dublin, Ireland

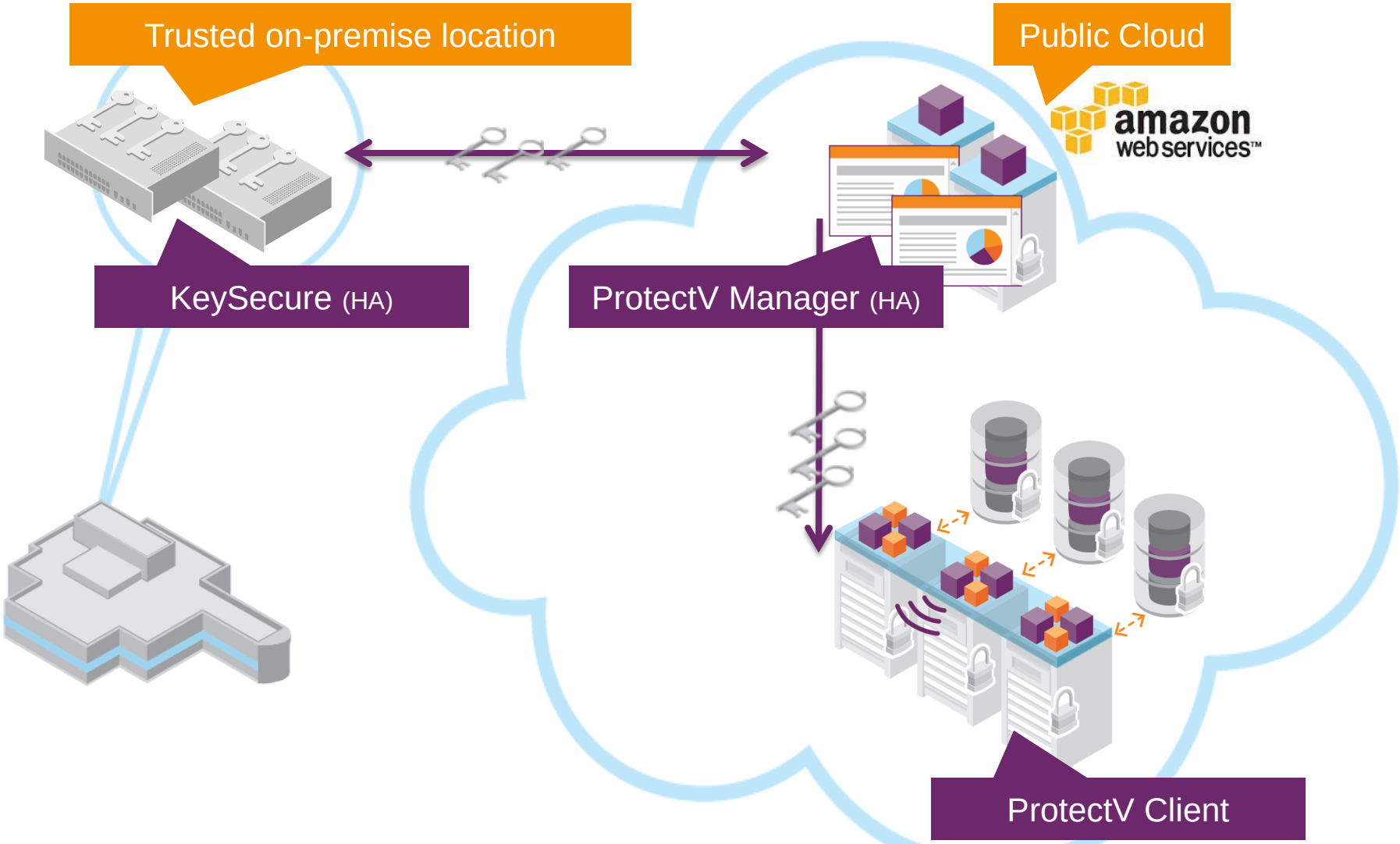
Customer Requirements

- Need to be compliant to Data Protection Directive of the European Union (95/46/EC) and German regulation to protect financial data (BDSG)
- Full redundant environment

Customer Profile

- HQ Zug, Switzerland, registered office in St Helier, Jersey
- Offices in 43 countries
- 8,500 employees
- Brands: AchieveGlobal, CRC Press, Datamonitor, ESI International Lloyd's List, Routledge and Taylor & Francis

INFORMA – AWS Deployment Scenario



SafeNet. THE DATA PROTECTION COMPANY

CASE STUDY

INFORMA - Multinational publishing & conference company

→ Project Outcome

- Even in a shared environment, assets remain encrypted and protected against exposure
- Security as an enabler for moving to the cloud
- Strengthened compliance
- Centralized control and management
- Transparent operations for end users

Crypto foundation and data encryption solutions applicable to MANY compliance mandates

PCI DSS 3.6, 4.1, 8.2, 8.4, 10.5 …

- **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data […]
- **4.1** protect sensitive cardholder data while in transit
- **8.2** In addition to assigning a unique ID, employ [... strong authentication ...] methods to authenticate all users
- **8.4** Render all passwords unreadable during transmission and storage on all system components using strong cryptography.
- **10.5** Secure audit trails so they cannot be altered.
- **3.1.1.b, 3.3, 4.2, 6.4.3/4, 6.5.3**, …

PCI DSS Cloud/Virtualization Guidelines

- **p. 32** Do not virtualize critical resources used in the generation of cryptographic keys
- **4.1.4 Implement defense in depth** […] consider how security can be applied to protect each technical layer, including but not limited to […] VMs, […] application, and data layers.

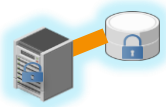
Beyond PCI DSS

- **EU privacy directives, EU 611/2013**
- **SOX, HIPAA, …**

Conclusion

Crypto Foundation

Deliver root of trust services for enterprise-wide data protection **DataSecure, KeySecure, Luna HSMs**



Structured Data Protection

Protect regulated data in databases and applications **Tokenization, ProtectDB, ProtectApp**

Unstructured Data Protection

Protect regulated data in files and storage **StorageSecure, ProtectFile**

Cloud Security

Assure ownership, isolation, and compliance of virtualized data **ProtectV**

- **Highly secure, robust, and flexible** infrastructure for data encryption
- **Ease compliance** with MANY regulations
  – PCI DSS, EU611/13, EU privacy regulation, and more
- **Field proven**

SafeNet. THE DATA PROTECTION COMPANY

SafeNet. THE DATA PROTECTION COMPANY

Thank You!